



# A multimodal liveness detection using statistical texture features and spatial analysis

Rohit Agarwal<sup>1</sup> · Anand Singh Jalal<sup>1</sup> · K. V. Arya<sup>2</sup>

Received: 30 July 2018 / Revised: 3 March 2019 / Accepted: 1 October 2019 /

Published online: 31 January 2020

© Springer Science+Business Media, LLC, part of Springer Nature 2020

## Abstract

Biometric authentication can establish a person's identity from their exclusive features. In general, biometric authentication can be vulnerable to spoofing attacks. Spoofing referred to presentation attack to mislead the biometric sensor. An anti-spoofing method is able to automatically differentiate between real biometric traits presented to the sensor and synthetically produced artifacts containing a biometric trait. There is a great need for a software-based liveness detection method that can classify the fake and real biometric traits. In this paper, we have proposed a liveness detection method using fingerprint and iris. In this method, statistical texture features and spatial analysis of the fingerprint pattern is utilized for fake or real classification. The approach is further improved by fusing iris modality with the fingerprint modality. The standard Haralick's statistical features based on the gray level co-occurrence matrix (GLCM) and Neighborhood Gray-Tone Difference Matrix (NGTDM) are used to generate a feature vector from the fingerprint. Texture feature from iris is used to boost the performance of the proposed liveness detection method. For the fusion Dempster-Shafer (D-S) approach is used at the decision level. Experiments have been performed on ATVS dataset and LivDet2011 dataset. The results show the convincing and effective outcomes of the proposed method.

**Keywords** Biometrics · Fingerprints · Iris · D-S Theory · Liveness detection · GLCM · NGTDM · Texture features

---

✉ Rohit Agarwal  
rohit.agrwal@gla.ac.in

Anand Singh Jalal  
asjalal@gla.ac.in

K. V. Arya  
kvarya@ietlucknow.ac.in

<sup>1</sup> Department of Computer Engineering and Applications, GLA University, Mathura, Uttar Pradesh, India

<sup>2</sup> Department of Computer Science & Engineering, IET Lucknow, Uttar Pradesh, India

## 1 Introduction

A biometric is used for automatic identification of an individual. Biometry technology is employed to acknowledge persons by using distinctive biological characteristics [27]. Biometric authentication is commonly applied the police investigation and forensic applications. In the last decade, the use of biometry is being hyperbolic day by day for human identification and verification. Biometry has benefits over standard authentication systems like a PIN and password based systems due to its individualism, permanence and the convenience of use. Numerous biometric traits (fingerprint, iris, palmprint, finger vein, finger knuckle, face, ear, hand pure mathematics etc.) are used for verification and identification. In a unimodal system, one biometric modality is employed for authentication, e.g., palm print, fingerprint, footprint, face, knuckle, voice, etc. However, unimodal biometry systems suffer from numerous inabilities to tolerate malformed information (noise, device, environmental noise, physical appearance), hence multiple biometric modalities can be used to improve the accuracy of a biometric [6].

An attack is the presence of a fabricated article or duplicate human attribute to a biometric system [22]. There are several attacks that can be imposed to compromise the security of a system. Ratha et al. [42] described these attacks and clubbed them into eight classes as shown in Fig. 1. In the proposed method attack 1 i.e. the presentation attack is considered.

Silicone, Playdoh and Gelatin are sensible materials to generate false distinctive finger impression on scanner [15, 46]. The sample can be captured of a fingerprint either from a supporting procedure or a non-helpful method. In an exceedingly useful procedure when the real user involves in the arrangement of the fake sample whereas in a non-agreeable method when the assaulter can catch the real one unknowingly. There are three types of spoofing attacks reported on the basis of which, an unauthorized person breaks any iris biometric system. These are photo attacks, contact-lens attacks and artificial eye attacks [14]. Numerous approaches are discussed in the literature to classify the fake and real person on the basis of contact-lens attack or photo attacks using texture features. Fingerprint and iris are widely used on the basis of the fact derived from Table 1.

Fingerprint and iris images show different textural characteristics between real and fake one. Spoof images show different behavior if they will be fetched with different sensing element or they are made of different fabrication [10]. The proposed system focuses on two objectives:

1. Investigation of robust liveness detection method using fingerprint and iris modality;
2. Decision level fusion to further improve the performance using multimodal biometric.

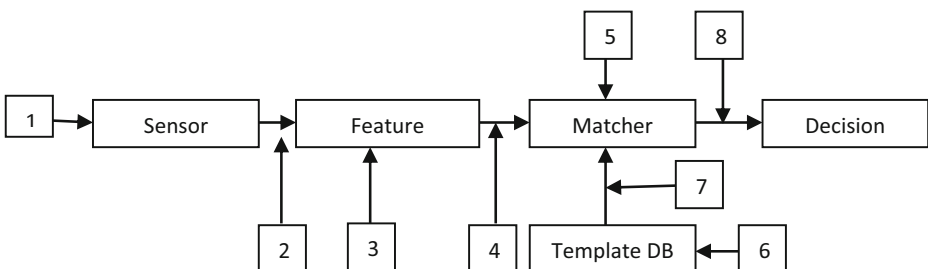


Fig. 1 Classification of attacks

**Table 1** Various biometric modalities performance [39]

Factors	Biometric Sensing System										
	Finger Print	Face	Hand Geometry	Iris	Voice	Signature	Gait	Ear	Palm Vein	Palm Print	
Accuracy	1	0	0.5	1	0.5	0.5	1	1	1	1	
Ease of Use	1	0.5	1	0.5	1	1	0.5	0.5	0.5	0.5	
Cost	0	0.5	0.5	1	1	0.5	0.5	1	1	1	
Privacy	1	1	0.5	1	1	1	1	0	0	0	
Distinctiveness	1	0	0.5	1	0	0.5	0.5	1	1	1	
Total	4	2	3	4.5	3.5	3	3.5	3.5	3.5	4	
Error Causing Factor	<b>Skin integrity</b>	<b>Pose &amp; Age</b>	<b>Injury</b>	<b>Eye Angle</b>	<b>Illness</b>	<b>Inconsistency</b>	<b>Weight Gain</b>	<b>Pose</b>	<b>Illness</b>	<b>Age</b>	

The proposed method is based on textural properties of real and fake biometric. In the proposed method, the fake fingerprint classification system is performed based on two types of texture properties. The primary category of texture uses statistical features and the second category uses macro-feature (core and delta) for fingerprint classification. To the best of our knowledge, no state-of-the-art methods supported core and delta points for fingerprint liveness detection. In the proposed method, fingerprint micro and macro texture features are consolidated and generate a single feature vector. For iris image classification, feature descriptor known as Local Binary Hexagonal Extrema Pattern (LBH<sub>x</sub>EP) [4] is used to extract the texture feature of iris. This proposed descriptor works efficiently in both types of attack i.e. printed iris attack and contact lens attack.

In the proposed method, the performance is further improved by fusing the decision of both the modalities i.e. fingerprint and iris. Several methods such as sum-rule [43] and kernel-based [5] are available for biometric information fusion at matching level and decision level. The choice of decision level fusion is effective when the individual system makes a distinctive decision about the identity of an individual. In the proposed work, we have used the standard D-S theory for fusion of fingerprint and iris at decision level.

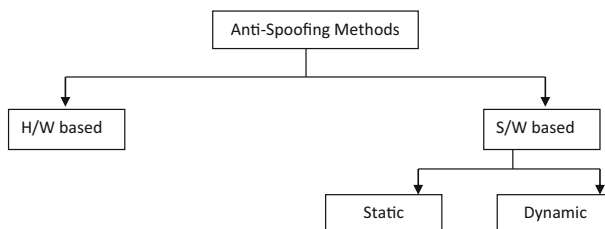
The proposed method is evaluated on a publicly ATVS and LivDet2011 datasets. The experimental results indicate 94.7% precision to arrange between the genuine and fake one for finger print. The decision level classification derives the prominent result using D-S theory when compared with sum- rule [28] and the product-based rule function [34] with 97.8% accuracy.

The rest of the paper is ordered as follows: Section 2 introduces the related work, Section 3 discusses the basic preliminaries used in the proposed system, Section 4 presents the proposed system, Section 5 presents the experimental results and comparison with state-of-the-art methods and Section 6 has conclusion of this paper.

## 1.1 Related work

In last few years many anti-spoofing or liveness detection algorithms have come to light which could classify between real and fake biometric sample. These algorithms can be classified into two classes: a) Hardware based and b) Software based. The classification is depicted in Fig. 2 [13].

Hardware-based solutions would like physical science gadgets. They are terribly expensive and are much addicted in to setting and skin state of affairs each. When we integrate the biometric with device then inclined outcome is obtained [7, 45]. Different electronic gadgets present different characteristics of same input image. Thus considering all this, we will focus on software solution supported static technique.



**Fig. 2** Classification of anti spoofing methods

Abhyankar and Schuckers [3] developed a detection technique that consisting of three parts: MTA, NRFA and fuzzy k-means classifier analysis. Classification rates of 97.3%, 96.5% and 92.3% were reportable for Optical, physical phenomenon DC and Electro-optical severally. The limitation of this work was that it fully was tested on restricted dataset and wishes the validity of technique against perspiration development across the population, also, not tested on completely different environmental conditions.

A technique for detection of pretend fingerprint that supports time-series photos given by Jia and Cai [29]. A fingerprint photo from time-series sequence is captured from a fingerprint scanner. The limitation of this technique was that it had been tested only restricted datasets and one device.

LBP (Local binary pattern), wavelet energy was used for feature extraction of fingerprint photos by Nikam and Agarwal [36]. Texture details are extracted by LBP and ridge frequencies and orientation details extracted from wavelet. Three classifiers were used for classification. Fingerprint databases consisting restricted dataset of gummy fingerprints.

In this strategy, Galbally et al. [16] have extracted 10 diverse quality measures as feature vector that will be utilized for description of fingerprint images. This technique does not consider any physiological changes. Nikam and Agrawal [37] gathered unique fingerprint images and investigate neighborhood and global information. Different classifiers KNN and neural system were likewise utilized for order.

A strategy for recognition of dynamic pores on distinctive finger impression photos for fake detection is planned by Memon et al. [33]. Strategy contains of high-pass separation, association separating and thresholding. The technique was tried on four edge esteems and constraint of this strategy that it does not decide ideal limit. Ridge -strength, Ridge-continuity and Ridge-clarity are extracted from an image proposed by Galbally et al. [17]. LDA (Linear Discriminate Analysis) classifier is used to classify between real or fake. A limitation is to find the best performing features subset and does not classify the samples based on other physiological measures.

Marasco and Sansone [32] conferred a method by combining sweat and morphology-based static highlights for distinctive finger impression aliveness recognition. A morphology-based methodology will separate amongst live and counterfeit footage, whereas sweat primarily based methodologies will derive dynamic information from a solitary image. The restriction of this work is that the highlights aren't chosen naturally for varied sensors.

A local phase quantization (LPQ) method is proposed by Ghiani et al. [20]. LPQ can distinguish spectrum differences between a "live" fingerprint and a "fake" one. They adopted the rotation invariant extension of LPQ because surface of sensor can produce different fingerprint orientation. A feature vector of 25 image quality measures given by Galbally& Marcel [19]. In this system complexity is too high and inclusions of temporal information are required.

Abhishek and Yogi [2] projected a unique technique for distinctive the phony fingerprints utilizing gelatin, Play-Doh and polymer molds and then forth. The delivery of details during a distinctive mark is attention-grabbing and utilized by the bulk of the distinctive finger impression acceptance calculations. This method was tried on the fingerprint verification competition datasets and declared precision over 85%.

Low level gradient features and texture features from Gabor wavelet using dynamic score level integration proposed by Dubey, Goh and Thing [12]. They are not able to classify cooperative fake user and non-cooperative user with real user and fail to identify the macro features. Convolutional Neural Networks (CNNs) proposed by Nogueira et al. [38] for spoof

fingerprint detection. They have used four different models: two CNNs pertained on natural images, classical local binary pattern approach and CNN with random weights. They did not consider different kind of datasets with different sensors.

Yuan, C. et al. [53] extracted features in light-weight of CNN and passed to SVM classifier. PCA is used to decrease the dimension when every convolutional or pooling activity done.

Fake iris detection system is strictly based on types of attack. Photo attack will behave differently as contact lens attack. Different approaches have been proposed by researchers by considering these types of attack. Galbally et al. [18] proposed a method with quality related features and applicable only on high quality iris printed images.

Galbally et al. [19] extracted feature vector of iris image from quality measures. LDA and QDA classifier are used to classify between real and fake. This method is applicable only for photo attack. Raghavendra and Busch [41] use M-BSIF for feature extraction. It is validating only on photo attack and decision level fusion is not tested. Zernike moments are calculated by Kohli et al. [31] across the iris image and LBPV is used for textural changes. It emphasizes on textural changes, not sufficient for structural changes. Hu et al. [26] constructed local regional parts and proposed a local descriptor for low level features. They failed to construct strong regional features and overlap to each other.

Bhogal et al. [9] calculated six IQM to discriminate real from fake in presentation attacks for classification of iris. Abate et al. [1] used Hough transform for iris localization and calculated 6 metrics for 32 sections, 4 rows and 8 columns. It is tested on UPOL, UBIRIS and MICHE dataset. This approach is not suitable for fake iris detection. Wang et al. [48] proposed quality assessment method for screen content images. A local information content weighting scheme issued to derive the optimal perceptual weights. This method is suitable for screen content images but not for real or finger print images and as well as not for real and fake iris images.

When the different biometric modalities are retrieved from different detector, then it may be from dissimilar scale or with dissimilar distribution. After multiple decisions from different platform, we have to take a final perception of the things by considering all separate decisions. Poh et al. [40] considered fingerprint and face images at decision level fusion. The outputs have been combined using the naive Bayes principal.

Vora et al. [47] focused on statistical analysis of different kernel methods. They used SVM based fusion of match scores for face and fingerprint biometric trait. Efficient multimodal biometric systems for face and iris fusion are proposed by Gomez-Barrero et al. [21]. They compute the similarity scores obtained by the face and iris and normalized scores are fused with a sum.

Dempster–Shafer theory used at score-level for multi-biometric detection proposed by Nguyen et al. [35] with uncertainty factors. D-S theory is implemented on score level and used for authentication. Wild et al. [49] proposed a method for fingerprint and face fusion in the presence of attacks. 1-median filtering is used at score level. Human ear and palm print are used in biometric recognition by Hezil and Boukrouche [25]. They used serial fusion method for features concatenation.

In the proposed system, statistical texture features and spatial analysis of the fingerprint pattern is utilized for fake or real classification. The approach is further improved by fusing iris modality with the fingerprint modality. In this paper, we are using decision level fusion using D-S theory and find the prominent result, when is implemented on ATVS, LivDet2011 and IIIT-D CLI dataset.

### 1.2 Preliminaries

In this section we will discuss the basic preliminaries used in the proposed system. Statistical texture feature i.e. micro features are derived from Gray Level Co-occurrence Matrix (GLCM) and are proposed by Haralick [8]. Haralick statistical features are good for micro textures; however, they show average performance on macro textures based on spatial analysis. Amadasun and King [24] proposed five macro texture features derived from Neighborhood Gray Tone Difference Matrix (NGTDM). D-S theory [44] is used for fusion of independent multi decision at decision level. On the basis of the final decision, proposed liveness detection approach decides the person is authentic or not. If the person is authentic then user will be accepted, otherwise rejected.

### 1.3 Neighborhood gray-tone difference matrix (NGTDM) [8]

NGTDM calculates the dissimilarity between a gray value and the average gray value of its neighbors within distance  $\delta$ . The sum of total differences for gray level  $i$ , is stored in the matrix. Let  $X_{gl}$  be a set of segmented voxels and  $x_{gl}(j_x, j_y, j_z) \in X_{gl}$  be the gray level of a voxel at position  $(j_x, j_y, j_z)$  then the average gray level of the neighborhood is:

$$\begin{aligned} \bar{A}_i &= \bar{A}(j_x, j_y, j_z) \\ &= \frac{1}{w} \sum_{k_x=-\delta}^{\delta} \sum_{k_y=-\delta}^{\delta} \sum_{k_z=-\delta}^{\delta} x_{gl}(j_x = k_x, j_y = k_y, j_z = k_z), \end{aligned} \tag{1}$$

Where  $(k_x, k_y, k_z) \neq (0, 0, 0)$  and  $x_{gl}(j_x = k_x, j_y = k_y, j_z = k_z) \in X_{gl}$  and  $w$  is the number of voxels in the neighborhood that are also in  $X_{gl}$ .

### 1.4 Gray level co-occurrence matrix (GLCM) [24]

The gray-level co-occurrence matrix, one of the most known texture analysis method related to second order statistics. Each entry of the matrix will represent number of occurrence of one pixel with intensity  $i$  and another pixel with intensity  $j$  at a separation  $D = 1, 2, 3, \dots$  toward the path  $\theta = 0^\circ, 45^\circ, 90^\circ, 135^\circ$  of an image  $I$ . In Equation 2,  $(L \times M)$  is the set of pixels of the image ordered by row-column,  $\#$  denotes number of elements in the set with intensity  $i$  and  $j$ .  $(\times 1, \times 2)$  and  $(\times 3, \times 4)$  are the ordered set of pixels.

$$\left. \begin{aligned} X(i, j, x, 0^\circ) &= \#\{((x1, x2), (x3, x3)) \in (L \times M) \times (L \times M) \\ &\quad : |x1-x3| = 0, |x2-x4| = D, I(x1, x2) = i, I(x3, x4) = j\} \\ X(i, j, x, 45^\circ) &= \#\{((x1, x2), (x3, x4)) \in (L \times M) \times (L \times M) \\ &\quad : (x1-x3 = D, x2-x4 = D) \\ &\quad \text{or } (x1-x3 = -D, x2-x4 = D), I(x1, x2) = i, I(x3, x4) = j\} \\ X(i, j, x, 90^\circ) &= \#\{((x1, x2), (x3, x4)) \in (L \times M) \times (L \times M) \\ &\quad : |x1-x2| = D, x3-x4 = 0, I(x1, x2) = i, I(x3, x4) = j\} \\ X(i, j, x, 135^\circ) &= \#\{((x1, x2), (x3, x4)) \in (L \times M) \times (L \times M) \\ &\quad : (x1-x2 = D, x3-x4 = D) \\ &\quad \text{or } (x1-x3 = -D, x2-x4 = -D), I(x1, x2) = i, I(x3, x4) = j\} \end{aligned} \right\} \tag{2}$$

The computation of GLCM at  $D = 1$  is described as follows.

<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td style="text-align: center;">0</td><td style="text-align: center;">0</td><td style="text-align: center;">1</td><td style="text-align: center;">1</td></tr> <tr><td style="text-align: center;">0</td><td style="text-align: center;">0</td><td style="text-align: center;">1</td><td style="text-align: center;">1</td></tr> <tr><td style="text-align: center;">0</td><td style="text-align: center;">2</td><td style="text-align: center;">2</td><td style="text-align: center;">2</td></tr> <tr><td style="text-align: center;">2</td><td style="text-align: center;">2</td><td style="text-align: center;">3</td><td style="text-align: center;">3</td></tr> </table> <p style="text-align: center;">(a) Image</p>	0	0	1	1	0	0	1	1	0	2	2	2	2	2	3	3	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td colspan="2" rowspan="2"></td> <th colspan="4">Gray Tone</th> </tr> <tr> <th>0</th><th>1</th><th>2</th><th>3</th> </tr> <tr> <th rowspan="4">Gray Tone</th> <th>0</th> <td>#(0,0)</td><td>#(0,1)</td><td>#(0,2)</td><td>#(0,3)</td> </tr> <tr> <th>1</th> <td>#(1,0)</td><td>#(1,1)</td><td>#(1,2)</td><td>#(1,3)</td> </tr> <tr> <th>2</th> <td>#(2,0)</td><td>#(2,1)</td><td>#(2,2)</td><td>#(2,3)</td> </tr> <tr> <th>3</th> <td>#(3,0)</td><td>#(3,1)</td><td>#(3,2)</td><td>#(3,3)</td> </tr> </table> <p style="text-align: center;">(b) General form of GLCM</p>			Gray Tone				0	1	2	3	Gray Tone	0	#(0,0)	#(0,1)	#(0,2)	#(0,3)	1	#(1,0)	#(1,1)	#(1,2)	#(1,3)	2	#(2,0)	#(2,1)	#(2,2)	#(2,3)	3	#(3,0)	#(3,1)	#(3,2)	#(3,3)
0	0	1	1																																													
0	0	1	1																																													
0	2	2	2																																													
2	2	3	3																																													
		Gray Tone																																														
		0	1	2	3																																											
Gray Tone	0	#(0,0)	#(0,1)	#(0,2)	#(0,3)																																											
	1	#(1,0)	#(1,1)	#(1,2)	#(1,3)																																											
	2	#(2,0)	#(2,1)	#(2,2)	#(2,3)																																											
	3	#(3,0)	#(3,1)	#(3,2)	#(3,3)																																											
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td rowspan="4" style="text-align: center; vertical-align: middle;"><math>P_H^{At 0^0}</math></td> <td style="text-align: center;">4</td><td style="text-align: center;">2</td><td style="text-align: center;">1</td><td style="text-align: center;">0</td> </tr> <tr> <td style="text-align: center;">2</td><td style="text-align: center;">4</td><td style="text-align: center;">0</td><td style="text-align: center;">0</td> </tr> <tr> <td style="text-align: center;">1</td><td style="text-align: center;">0</td><td style="text-align: center;">6</td><td style="text-align: center;">1</td> </tr> <tr> <td style="text-align: center;">0</td><td style="text-align: center;">0</td><td style="text-align: center;">1</td><td style="text-align: center;">2</td> </tr> </table> <p style="text-align: center;">(c)</p>	$P_H^{At 0^0}$	4	2	1	0	2	4	0	0	1	0	6	1	0	0	1	2	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td rowspan="4" style="text-align: center; vertical-align: middle;"><math>P_V^{At 90^0}</math></td> <td style="text-align: center;">6</td><td style="text-align: center;">0</td><td style="text-align: center;">2</td><td style="text-align: center;">0</td> </tr> <tr> <td style="text-align: center;">0</td><td style="text-align: center;">4</td><td style="text-align: center;">2</td><td style="text-align: center;">0</td> </tr> <tr> <td style="text-align: center;">2</td><td style="text-align: center;">2</td><td style="text-align: center;">2</td><td style="text-align: center;">2</td> </tr> <tr> <td style="text-align: center;">0</td><td style="text-align: center;">0</td><td style="text-align: center;">2</td><td style="text-align: center;">0</td> </tr> </table> <p style="text-align: center;">(d)</p>	$P_V^{At 90^0}$	6	0	2	0	0	4	2	0	2	2	2	2	0	0	2	0													
$P_H^{At 0^0}$		4	2	1	0																																											
		2	4	0	0																																											
		1	0	6	1																																											
	0	0	1	2																																												
$P_V^{At 90^0}$	6	0	2	0																																												
	0	4	2	0																																												
	2	2	2	2																																												
	0	0	2	0																																												
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td rowspan="4" style="text-align: center; vertical-align: middle;"><math>P_{LD}^{At 135^0}</math></td> <td style="text-align: center;">2</td><td style="text-align: center;">1</td><td style="text-align: center;">3</td><td style="text-align: center;">0</td> </tr> <tr> <td style="text-align: center;">1</td><td style="text-align: center;">2</td><td style="text-align: center;">1</td><td style="text-align: center;">0</td> </tr> <tr> <td style="text-align: center;">3</td><td style="text-align: center;">1</td><td style="text-align: center;">0</td><td style="text-align: center;">2</td> </tr> <tr> <td style="text-align: center;">0</td><td style="text-align: center;">0</td><td style="text-align: center;">2</td><td style="text-align: center;">0</td> </tr> </table> <p style="text-align: center;">(e)</p>	$P_{LD}^{At 135^0}$	2	1	3	0	1	2	1	0	3	1	0	2	0	0	2	0	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td rowspan="4" style="text-align: center; vertical-align: middle;"><math>P_{RD}^{At 45^0}</math></td> <td style="text-align: center;">4</td><td style="text-align: center;">1</td><td style="text-align: center;">0</td><td style="text-align: center;">0</td> </tr> <tr> <td style="text-align: center;">1</td><td style="text-align: center;">2</td><td style="text-align: center;">2</td><td style="text-align: center;">0</td> </tr> <tr> <td style="text-align: center;">0</td><td style="text-align: center;">2</td><td style="text-align: center;">4</td><td style="text-align: center;">1</td> </tr> <tr> <td style="text-align: center;">0</td><td style="text-align: center;">0</td><td style="text-align: center;">1</td><td style="text-align: center;">0</td> </tr> </table> <p style="text-align: center;">(f)</p>	$P_{RD}^{At 45^0}$	4	1	0	0	1	2	2	0	0	2	4	1	0	0	1	0													
$P_{LD}^{At 135^0}$		2	1	3	0																																											
		1	2	1	0																																											
		3	1	0	2																																											
	0	0	2	0																																												
$P_{RD}^{At 45^0}$	4	1	0	0																																												
	1	2	2	0																																												
	0	2	4	1																																												
	0	0	1	0																																												

### 1.5 Dempster-Shafer theory (D-S theory) [44]

D-S is a mathematical approach to combine evidences based on belief function and plausibility. Dempster-Shafer theory is an approach. Each fact has a degree of support, between 0 (no support for the fact) and 1 (full support for the fact). This Theory differs from Bayesian approach in a way it uses “Dempster’s rule of combination” to incorporate new information and can be considered a generalization of Baye’s rule. This theory also maintains a dual concept of weight.

Let  $\Theta$  be a set of possible conclusions:  $\Theta = \{f_1, f_2, \dots, f_n\}$ . Each  $f_i$  is mutually exclusive and  $\Theta$  is exhaustive.

#### 1.5.1 Frame of discernment

The frame of discernment of  $\Theta$  is the set of all possible subsets of  $\Theta = \{f_1, f_2, f_3\}$ . Then the frame of discernment of  $\Theta$  is:

$$\{\emptyset, f_1, f_2, f_3, \{f_1, f_2\}, \{f_1, f_3\}, \{f_2, f_3\}, \{f_1, f_2, f_3\}\}$$

$\emptyset$  has a probability of 0. The element in the power set has a probability between 0 and 1 and the probability of  $\{f_1, f_2, f_3\}$  is 1.

#### 1.5.2 Mass function

It is a function represented as  $m(A)$  that gives a value between [0, 1] to each focal element A. It is based on the evidence. The value 0 represents no belief and value 1 demonstrates total belief and is allocated to every subset of the power set. If mass function of an individual proposition



of A is  $m(A)$  then it is given in Equation 3:

$$\sum_{A \subset \theta} m(A) = 1 \tag{3}$$

### 1.5.3 Belief and plausibility of A

The belief in an element A is the sum of the masses of elements which are subsets of A is represented as Equation 4.

$$Bel(A) = \sum_{B \subset A} m(B) \tag{4}$$

The plausibility  $pl(A)$  is the sum of all the masses of the sets that intersect with the set given in Equation 5.

$$pl(A) = 1 - Bel(\neg A) = \sum_{B \cap A \neq \emptyset} m(B) \tag{5}$$

### 1.6 Belief interval of A

The confidence associated with set A is defined by the belief interval:

$$[bel(A) \ pl(A)]$$

The probability lies between  $bel(A)$  and  $pl(A)$ . Probability cannot be less than  $bel(A)$  and  $pl(A)$  represents the maximum possible value of  $prob(A)$ . A small difference between  $bel(A)$  and  $pl(A)$  shows the certainty about our belief and large difference shows the uncertainty about our belief.

### 1.7 Dempster rule of combination

The mass of focal element is combined by using following rule of combination:

$$m_{final} = m1 \oplus m2 \oplus m3 \oplus m4$$

Where

$$[m(A) \oplus m(B)] = m(c) = \frac{\sum_{A \cap B = C} m(A)m(B)}{1 - \sum_{A \cap B = \varphi} m(A)m(B)} \tag{6}$$

### 1.8 Support vector machine (SVM) classifier [52]

We have used Support Vector Machine (SVM) [52] as a classifier to classify fingerprints into live and fake classes since it provides an effective result for real time applications. We have a tendency to pass training feature set and testing feature set to the SVM classifier wherever it classifies to the

tested fingerprint pictures into fake and live class. SVM uses different kernel mapping functions like linear, polynomial and Gaussian, etc. that transforms a feature vector into another high dimensional area. In the proposed system we use linear kernel for fingerprint and iris classification.

## 2 Proposed multimodal Liveness detection frameworks

Unimodal liveness detection systems are less secure and have unsatisfactory detection. New unnoticed materials and methods continuously challenged state-of-the-art spoofing detectors in a unimodal detection system. The major issue with unimodal liveness detection system is that no single technology is suitable for all the applications. Therefore, in this paper, we have proposed a multimodal liveness detection method that can be used to compensate the limitations of a unimodal liveness detection system. The proposed system has less FTA (failure-to-acquire), FTE (failure-to-enroll), FNMR (false non-match rates) and FMR (false match rate). The proposed method reduces data distortion and increased reliability.

The proposed multimodal liveness detection method is shown in Fig. 3. The proposed method consists of three modules. The first module describes a fingerprint liveness detection approach. The second module demonstrates iris liveness detection. Finally, a decision level fusion is implemented in the third module.

### 2.1 Fingerprint Liveness detection approach

The spoof fingerprint liveness detection is taken into account as a two-class classification i.e. real or fake. Real and fake fingerprint pictures possess different textures properties [13]. In this module, a feature vector consisting of texture features is utilized for classification by a support vector machine to classify input fingerprint image. The block diagram of the fingerprint liveness detection approach is shown in Fig. 4.

### 2.2 Preprocessing

The preprocessing step is used to enhance the image appearance and remove the unrelated noise from an image. In this work, to improve the contrast of the input image  $I$ , histogram equalization is performed:

$$H_{i,j} = \left[ (L-1) \sum_{n=0}^{I_{i,j}} NH_n \right] \quad (7)$$

Where  $H$  is the histogram equalized image,  $L$  is the possible intensity value and  $NH$  denote the normalized histogram.

### 2.3 Extraction of feature vector

A) The spatial analysis is performed by using following global macro features from NGTDM proposed by Amadasun [8].

1. Resized the fingerprint image into  $128 \times 128$  pixels.

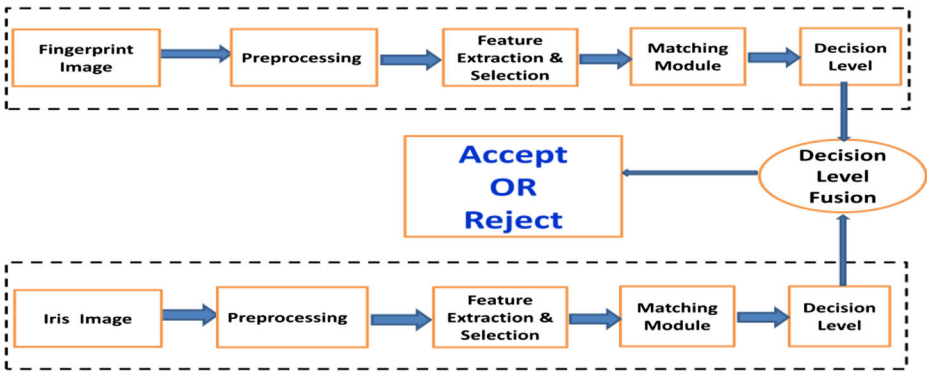


Fig. 3 Framework of proposed multimodal detection system

2. Find the different NGTDM using  $d = 1$  for each individual finger print image.
3. Calculate the following two global texture features from NGTDM:

- Coarseness: The quality of being rough or harsh.
- Busyness: Level of busyness is measured in terms of spatial magnitude of intensity changes.

B) To extract the statistical texture features from GLCM, following steps are taken:

1. Compute four normalized GLCM matrices from the processed fingerprint image of  $M = 128 \times 128$  at distance  $d = 1$ , in the direction  $\theta = 0^\circ, 45^\circ, 90^\circ, 135^\circ$ .
2. Find out a single matrix by taking the averages of all the four normalized GLCM matrices.
3. Slide a window of size  $m \times m$  pixels over the GLCM matrix of  $128 \times 128$  with a translation step  $t = m/2$  pixels. In our experiments we have taken  $m = 16$ . The number sub images are computed as follows:

$$N = \lceil \text{floor}((M-m)/t) + 1 \rceil^2 \tag{8}$$

4. For each sub image, calculate the following six local Haralick features [24]:

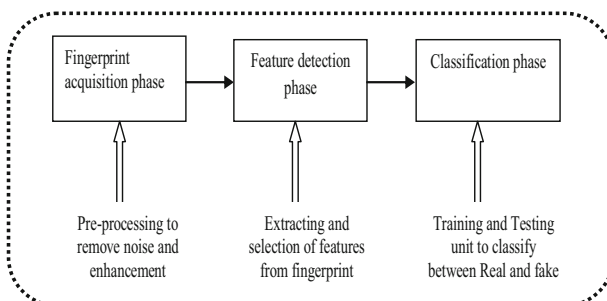


Fig. 4 Framework of fake fingerprint detection system

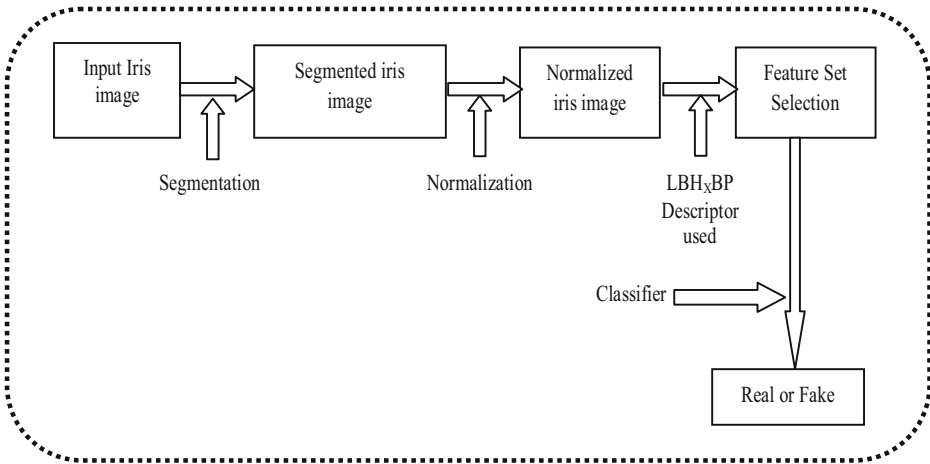


Fig. 5 Framework of fake iris detection system

- Energy: It deals with the smoothness of the image.
- Contrast: Measures of local level variations of contrast.
- Correlation: Measures of correlation between pixels in two dissimilar directions.
- Variance: Measures contextual information i.e. dispersion around the mean of combinations of reference & neighbor pixels.
- Homogeneity: Measures that takes high esteems for low-differentiate pictures.
- Entropy: Measures of mediation and takes low esteems for smooth pictures.

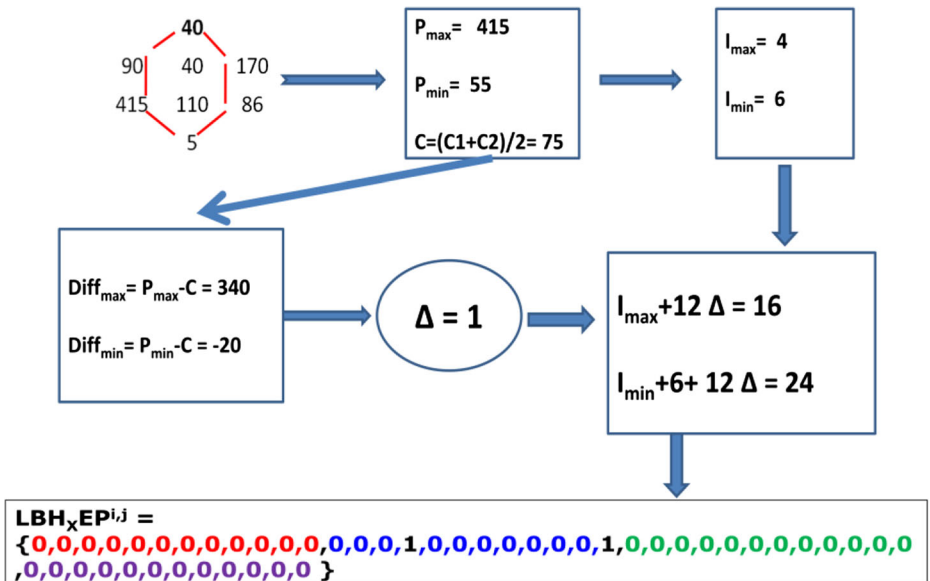


Fig. 6 LBH<sub>x</sub>EP<sup>i,j</sup> Computation

**Table 2** Structure of the ATVS-FFp

Sensors	Training (Real/ Fake)	Testing (Real/ Fake)	Types
S1	27/27	245/245	Cooperation
S2	27/27	245/245	
S3	27/27	245/245	
S1	26/26	230/230	Without-cooperation
S2	26/26	230/230	
S3	26/26	230/230	
S1	20/20	180/180	Cross-validation
S2	20/20	180/180	
S3	20/20	180/180	

## 2.4 Iris Liveness detection approach

This is a classification problem, which is used to differentiate between real and fake iris images. The block diagram is given in Fig. 5 and this module consists of the following steps.

- Segmentation of iris image using integro-differential operator [11].
- Daugman's rubber sheet model used for normalized the iris image [30].
- Extract iris features using  $LBH_xBP$  descriptor [4].
- Classification done by using SVM classifier.

In the proposed module for iris fake detection, a feature descriptor known as Local Binary Hexagonal Extrema Pattern ( $LBH_xEP$ ) [4] is used. The objective of the descriptor is to extract a feature vector from normalized iris image. In this descriptor, we find the extrema (maximum and minimum) values and indexes from the local Hexagonal pattern and find the average of two center pixels in hexagonal pattern. We derived the relationship between one center pixel and all 6-neighbors at distance 1 and 2. The intensity values of the local hexagonal extrema are compared with the intensity value of the center pixel. The  $LBH_xEP$  over the normalized iris image  $M$  is given calculated using Equation 9.

$$LBH_xEP = \frac{1}{n} * \sum_{i=1}^n LBH_xEP_i \quad (9)$$

Where  $n$  is the number of sub images and the Local Binary Hexagonal Extrema Pattern ( $LBH_xEP_i$ ) for one local pattern is calculated as shown in Fig. 6.

## 3 Multimodal fusion using Dempster-Shafer theory

In a multimodal biometric system, the biometric information is captured from different biometric modalities and from different sensors. The decision level fusion strategy integrates biometric traits in an exceedingly easy as compared with feature level fusion, which typically directly integrates totally different biometric traits at the feature level. Fusion is performed at a

**Table 3** Structure of the ATVS-Fir DB

Sensor	Training set (Live/Spoof)	Testing set (Live/Spoof)
LG IrisAccess EOU3000	300/300	425/425

**Table 4** Structure of the LivDet2011 dataset

Sensors	Training set(Live/Spoof)	Testing set (Live/Spoof)
Biometrica	500/500	500/500
Digital Persona	502/502	500/500
Italdata	500/500	500/500
Sagem	504/504	500/500

later stage in decision level, as compared to the multi-biometric system at feature level fusion or matching score level fusion methods. In the proposed system, each biometric modality is classified independently and the final classification is done by fusing the decision of two modalities i.e. fingerprint and iris, at decision level using D-S theory. In the proposed method, we define the two frame of discernment:

$$\Theta_f = \{\theta_{fr}, \theta_{fi}\}$$

$$\Theta_i = \{\theta_{ir}, \theta_{ii}\}$$

Where  $\theta_{fr}$  and  $\theta_{fi}$  represent the real and imposter classes in finger and  $\theta_{ir}$ ,  $\theta_{ii}$  represent the real and imposter classes in iris respectively. The decision level fusion is implemented by the following steps:

- 1) To convert the genuine predictive value and imposter predictive value for finger and iris into evidence in the range  $[0, 1]$ .

$$m_i(\theta_{ij}) = \psi(S_i) \quad (10)$$

where  $i$  corresponds to the fingerprint and iris, and  $j$  represents genuine or imposter,  $S_i$  is the genuine and imposter average error rate (AER) value, by the classifier  $i$ . In the proposed method, sigmoid transform function is used and given as in Equation 11:

$$\psi(s_i) = 1/(1 + \exp^{-S_i}) \quad (11)$$

- 2) Combine all evidences for all focal elements for  $m_f$  and  $m_i$  using D-S rule of combination for the following frame using Equation 12.

$$\{\phi, \theta_{fg}, \theta_{fi}, \theta_{ig}, \theta_{ii}, \{\theta_{fg}, \theta_{ig}\}, \{\theta_{fg}, \theta_{ii}\}, \{\theta_{fi}, \theta_{ig}\}, \{\theta_{fi}, \theta_{ii}\}\}$$

$$m_{fusion}(\theta_{ij}) = m_f(\theta_{ij}) \oplus m_i(\theta_{ij}) \quad (12)$$

**Table 5** Structure of the IIIT-D CLIdataset

Sensor	Training set (Live/Spoof)	Testing set (Live/Spoof)
Cognet	202/202	450/450
Vista	202/202	450/450

**Table 6** Structure of the paired dataset

Modalities	Training set Live/Spoof	Testing set Live/Spoof
Fingerprint and iris	50/50	100/100

3) Calculate belief and plausibility to all focal elements of finger and iris.

$$Bel(A_{fi}) = \sum_{B \subset A} m(B) \tag{13}$$

$$pl(A_{fi}) = \sum_{B \cap A \neq \emptyset} m(B) \tag{14}$$

4) Proposed liveness detection is two class problem (Accept, Reject) and final result is obtained by applying threshold t:

$$\text{Result} = \begin{cases} \text{Accept} & t \geq [bel(A) - pl(A)] \\ \text{Reject} & \text{otherwise} \end{cases} \tag{15}$$

### 4 Results and discussion

This section describes the analysis of classification by the proposed system for liveness detection. To estimate the effectiveness and accuracy of the proposed system, we have compared the results of the proposed system with existing methods. The proposed system is implemented in MATLAB 8.3.0.532(R2016a) at Intel® core™ i7 CPU @ 2.2 GHz with 8 GB of RAM. The experimental results are depicted in the form of graphs and tables.

**Table 7** AER value and Accuracy for cooperative, non-cooperative and cross dataset

Sensors	Performance Criteria		Types
	AER	ACA(%)	
S1	2.50	97.10	Cooperative
S2	1.94	97.43	
S3	2.24	97.17	
S1	2.39	92.96	Non-cooperative
S2	2.43	91.61	
S3	3.88	92.06	
S1	12	86.58	Cross Validation
S2	9.8	88.82	
S3	9.5	90.49	

**Table 8** AER value and ACA for LivDet2011 dataset

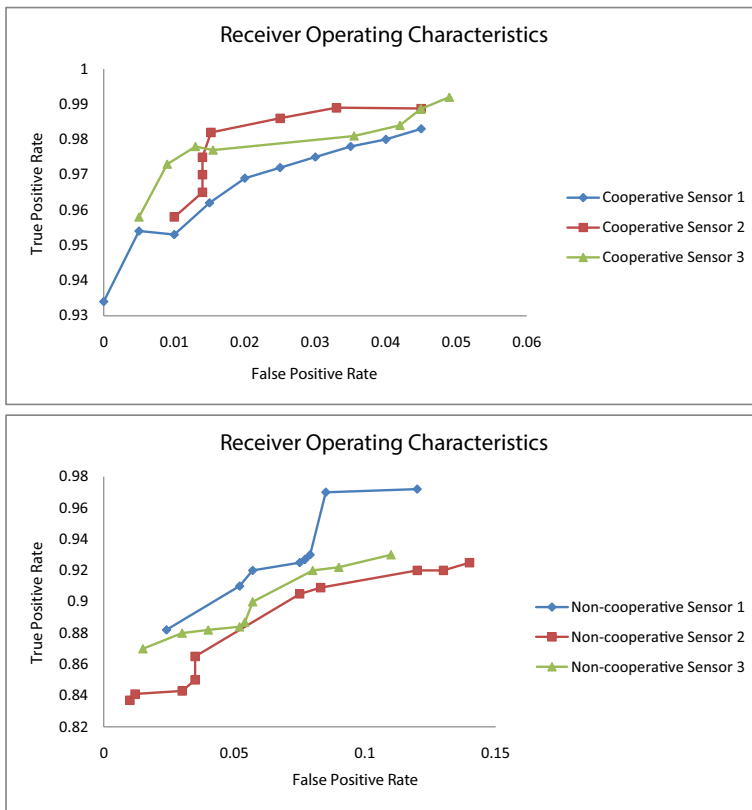
Sensors	AER	ACA
Biometrica	3.2	93.70
Digital Persona	3.5	92.05
Italdata	3.6	93.75
Sagem	2.7	95.20

### 4.1 Dataset

The performance of the proposed system is tested on the standard datasets ATVS-FFp [17], ATVS-Flr [17], LivDet2011 [51] and IIID-CLI database [50]. As far as our knowledge is concerned there is no spoof dataset which has multi traits for the same person. In the proposed system, a virtual user is considered and organic dataset for that user is created by pairing fingerprint and iris images from the available dataset for the multimodal liveness detection system.

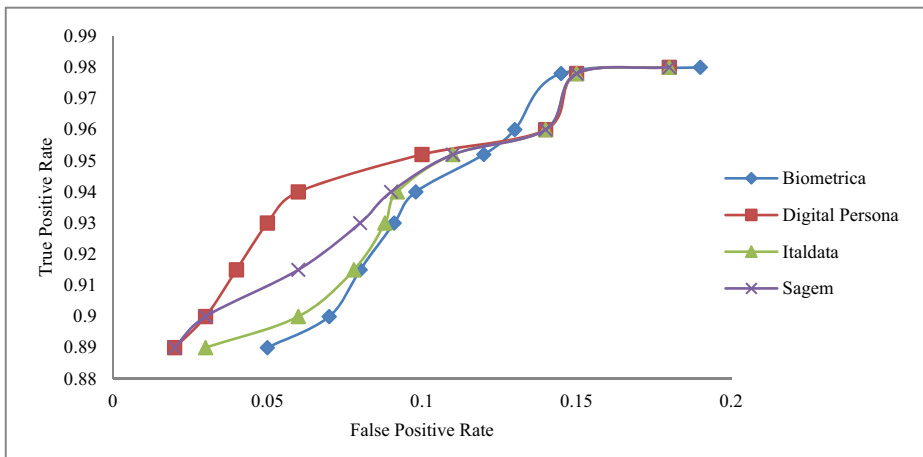
#### 4.1.1 ATVS-FFp dataset [17]

Two types of the dataset are used in the ATVS-FFp. The first dataset is prepared with the cooperation of the user and second is without the cooperation of the user. In the first dataset,



**Fig. 7** ROC curve between sensors of cooperative dataset and non-cooperative dataset of ATVS dataset





**Fig. 8** ROC curve between Sensors of LivDet2011 dataset

index and mid fingers for the left and right hands of 17 subjects are taken. In this dataset three sensors named as Precise SC100 (S1), BiometrikaFX2000 (S2) and Yubee (S3) are used. The database consists of 816 real and spoofed image samples.

The second dataset contains 768 real images and the same number of fake images of 16 persons. For cross-validation, we have reconstituted the third dataset from the ATVS-FFp dataset, where we mix the entire sample from both cooperative and non-cooperative fingerprint images. In Table 2 structure of ATVS-FFp dataset is demonstrated.

#### 4.1.2 ATVS-FIir dataset [17]

In this dataset printed images of the real and fake iris of 50 users have been taken. It comprises 800 fake and real iris images. The real and fake samples of iris were captured using only one sensor. Table 3 represents the structure of ATVS-FIir dataset.

#### 4.1.3 LiveDet2011 dataset [51]

This dataset is created during spoof fingerprint detection competition held in 2011. Four sensors (Biometrika, Digital Persona, Italdata and Sagem) are used to extract the iris images. Six unique materials known as gelatin, latex, PlayDoh, silicone, ecoflex and wood are used to manufacture fake fingerprint. Structure of the LivDet2011 is shown in Table 4.

**Table 9** Comparison between AER on Biometrika Sensor

Approaches	AER
Galbally et al. [17]	5.8
Dubey et al. [12]	2.27
Proposed System	2.19

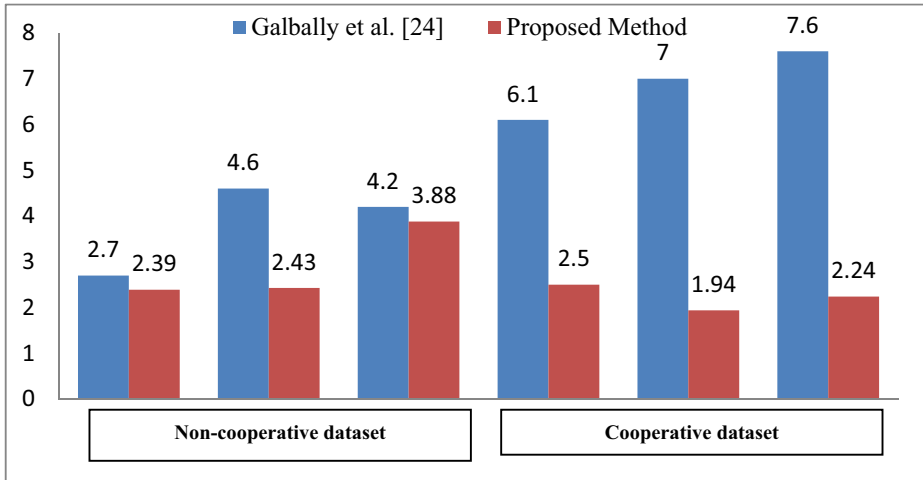


Fig. 9 Comparison between AER of proposed system with Galbally et al. [17]

#### 4.1.4 IIIT-D CLI dataset [50]

In this dataset, left and right iris images of 101 are captured with 202 iris classes. Total of 6570 iris images are captured. Two iris sensors i.e. Cognet and Vista are used for extraction. Table 5 is used to represent the structure of IIIT-D CLI dataset.

#### 4.1.5 Paired dataset

This organic paired database is created for multimodal liveness detection from two different modalities i.e. fingerprint and iris modalities of different users from ATVS-FFp

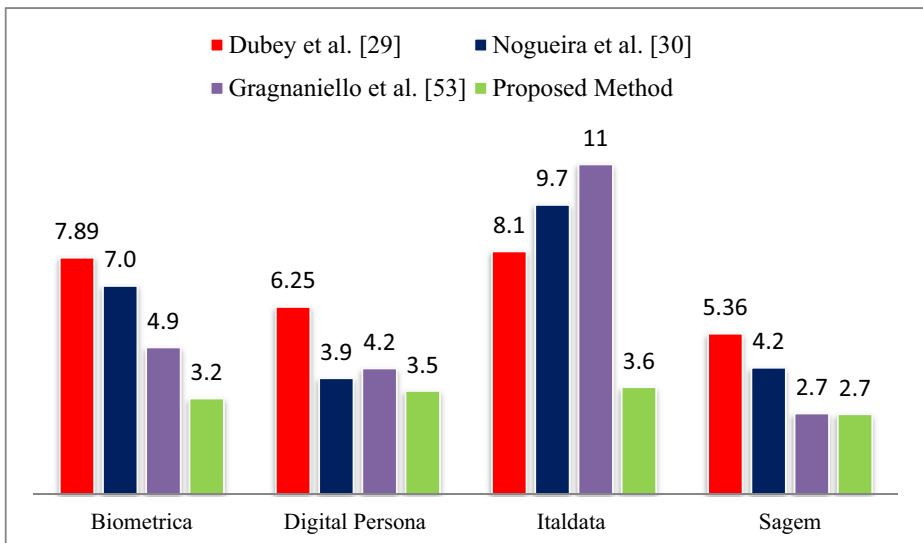


Fig. 10 Comparison between AER of proposed system with others tested on LivDet2011 dataset

**Table 10** ACA of proposed system with state-of-the-art approaches

Approaches	ACA
Galbally et al. [17]	90
Galbally et al. [19]	92
Abhishek and Yogi [2]	85
Proposed System	94.7

and ATVS-Fir datasets. A chimeric dataset is compiled by pairing iris and fingerprint images from different datasets. This chimeric dataset consists of 150 virtual users with 150 samples of real and fake fingerprint and iris images. Table 6 illustrates the test dataset for fusion at decision level.

## 4.2 Evaluation measures

The proposed method is validated using the following evaluation measures:

$$\text{Average Error Rate (AER)} = (\text{FAR} + \text{FRR})/2 \quad (16)$$

Where

$$\text{False Accept Rate (FAR)} = \frac{(\text{No. of accepted imposters as real}) \times 100}{(\text{Total no. of imposters})} \quad (17)$$

and

$$\text{False Reject Rate (FRR)} = \frac{(\text{No. of rejected reals as imposter}) \times 100}{(\text{Total no. of reals})} \quad (18)$$

AER is calculated from FAR and FRR and average classification accuracy (ACA) is the criteria to assess the reliability of a biometric modality. The less value of AER and the high value of ACA denote the good performance of the system.

$$\text{Average Classification Accuracy (ACA)} = \frac{(\text{Correct real rate} + \text{Correct fake rate})}{2} \quad (19)$$

## 4.3 Experiments on fingerprint dataset

In the first experiment, we have analyzed the AER and ACA value for different sensors using ATVS-FFp dataset and LiveDet 2011 dataset. Table 7 illustrates the AER and ACA for cooperative, non-cooperative and cross-validation dataset on three sensors. It is concluded from the results that for a cooperative dataset, Sensor S2 performs better than other two sensors

**Table 11** Impact of threshold on AER

Threshold	0.001	0.002	0.003	0.004	0.005
AER	2.23	2.01	1.93	1.8	1.19

**Table 12** AER performance of different approaches

Approaches	AER
Fingerprint Liveness Detection System	2.19
Iris Liveness Detection System	1.80
Proposed Multimodal Liveness Detection System	1.19

and for cross-validation Sensor S3 is better than the other two. Table 8 shows AER value and ACA value of Sensor Sagem outperform than the other three sensors.

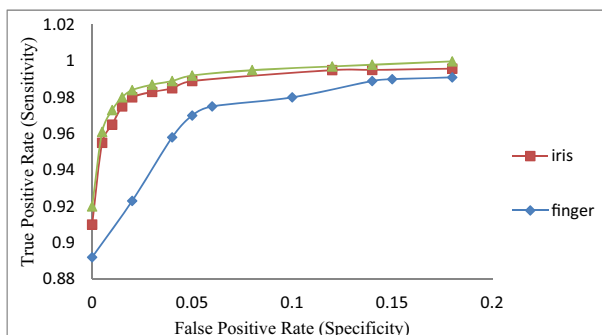
To further validate the performance a Receiver Operating Characteristics (ROC) curve between False Positive Rate (FPR) and True Positive Rate (TPR) for ATVS-FFp dataset is also analyzed. ROC curves are used to show in a graphical way the connection/trade-off between sensitivity and specificity for every possible test. The area under the ROC curve gives an idea about the benefit of testing. Figure 7 shows that sensor S2 and Sensor S1 is more effective for a cooperative dataset and non-cooperative dataset respectively. Figure 8 validates the performance of the proposed system on LivDet 2011 dataset.

Table 9 describes the relative comparison of AER between the proposed system and state-of-art methods [12, 17] on the ATVS dataset. We can strongly conclude that the proposed system is more efficient than the other two state-of-the-art systems.

To further validate the performance of the proposed system, we compare the AER value of the proposed system with Galbally et al. [17] on a cooperative dataset and non-cooperative dataset. The Sensor S2 is equipped with a 32-bit RISC processor and implements very reliable symmetric encryption algorithms with 128-bit keys. Besides the resolution and the size of the sensing area, the images produced by a fingerprint scanner are characterized by other factors which conclude their contrast and geometric distortion. The texture features used in the proposed system suppress these distortions and produce a robust feature vector for effective liveness detection. Figure 9 demonstrates that the proposed system shows low AER for Sensor S2 on cooperative dataset and low AER for Sensor S1 on non-cooperative dataset.

Figure 10 shows the relative comparison of AER between the proposed method and state-of-the-art methods [12, 23, 38] on the LivDet2011 dataset. It is depicted from Fig. 10 that the proposed system is competent and effective as compared state-of-the-art systems.

Table 10 illustrates the ACA of the different state-of-the-art liveness detection system. It is evident from the analysis that the proposed system has a higher accuracy i.e. 94.7% for both fake and real fingerprint liveness detection system, which is comparatively better than other related works.

**Fig. 11** ROC curve between unimodal systems and multimodal system

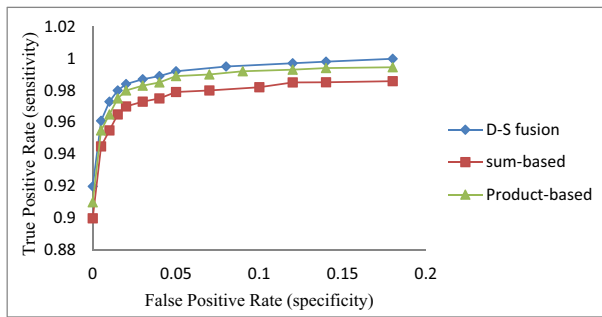


Fig. 12 ROC curve between D-S fusion and other quality based fusion

#### 4.4 Analysis of multimodal liveness detection system

After fusing the decision from fingerprint and iris liveness detection, a threshold is applied to produce effective decision result. The impact of the threshold on the liveness detection performance is illustrated in Table 11.

The proposed D-S fusion approach is measured on AER, which incorporates both FAR and FRR for finger liveness detection system and iris liveness detection system. In the proposed system organic dataset is used. AER performance of unimodal detection system with multimodal detection system is shown in Table 12.

The performance of the proposed method is also validated using ROC curve analysis as shown in Fig. 11. ROC curve represents the complete sensitivity/specificity report. It is an elementary tool for diagnostic test estimation. In a ROC curve, the true positive rate (Sensitivity) is plotted in function of the false positive rate (Specificity). Each point on the ROC curve represents a sensitivity/specificity pair. The area under the ROC curve (AUC) is a measure of how well a parameter can distinguish between two classifications i.e. real or fake. D-S based fusion approach achieve better performance over the individual modality i.e. fingerprint and iris detection system.

We have further demonstrated the performance of the proposed method against quality based approaches i.e. sum-based and product-based. Figure 12 demonstrates the D-S fusion is better than the other two fusion methods i.e. sum-based and product-based.

The performance of the proposed D-S fusion based approach in term of ACA is described in Table 13. It is concluded that the proposed system behaves better than other state-of-the-art methods and unimodal liveness system.

Table 13 ACA performance of different approaches

Approaches	ACA
Fingerprint Liveness Detection System	94.7
Iris Liveness Detection System	96.3
P. Wild et al. [49]	84
N. Hezil et al. [25]	80.53
Proposed Liveness Detection System	97.8

## 5 Conclusion

Liveness detections are methods to identify presentation attack by differentiating a real and fake biometric representation. In the proposed work, we have investigated the effectiveness of texture features for the liveliness detection system. The proposed method was further improved by fusing independent decision of individual modalities i.e. fingerprint and iris. The standard D-S theory is used for decision level fusion. The performance of the proposed method is tested on different standard datasets. The experimental results illustrate the effectiveness of the proposed approach and can improve the security level and reliability of any biometric system.

## References

1. Abate AF, Barra S, Casanova A, Fenu G, Marras M (2018) Iris quality assessment: a statistical approach for biometric security applications. In: International symposium on cyberspace safety and security. Springer, Cham, pp 270–278
2. Abhishek K, Yogi A (2015) A minutiae count based method for fake fingerprint detection. *Proc Comput Sci* 58:447–452
3. Abhyankar A, Schuckers S (2006) Fingerprint liveness detection using local ridge frequencies and multiresolution texture analysis techniques. In: Proceedings of IEEE international conference on image processing, pp 321–324
4. Agarwal R, Jalal AS, Arya KV (2018) Local binary hexagonal extrema pattern (LBHXEP): a new feature descriptor for fake IRIS detection. *Wireless personal communication: communicated*
5. Aguilar JF, Garcia JO, Rodriguez JG, Bigun J (2004) Kernel-based multimodal biometric verification using quality signals. In: Proceedings of SPIE biometric technology for human identification 5404, pp 544–554
6. Ahmad SMS, Ali BM, Adnan WAW (2012) Technical issues and challenges of biometric applications as access control tools of information security. *Int J Innov Comput Inf Control* 8(11):7983–7999
7. Al-Ajlan A (2013) Survey on fingerprint liveness detection. In: Proceedings of IEEE international workshop on biometrics and forensics (IWBF), pp 1–5
8. Amadasun M, King R (1989) Textural features corresponding to textural properties. *IEEE Trans Syst Man Cybern* 19(5):1264–1274
9. Bhogal APS, Söllinger D, Trung P, Uhl A (2017) Non-reference image quality assessment for biometric presentation attack detection. In: Proceedings of IEEE 5th international workshop on biometrics and forensics (IWBF), pp 1–6
10. Coli P, Marcialis GL, Roli F (2007) Vitality detection from fingerprint images: a critical survey. In: Proceedings of international conference on biometrics. Springer, Berlin/Heidelberg, pp 722–731
11. Daugman, J.,(2009) How iris recognition works. In: *The essential guide to image processing*, pp 715–739
12. Dubey RK, Goh J, Thing VL (2016) Fingerprint liveness detection from single image using low-level features and shape analysis. *IEEE Trans Inf Forensics Secur* 11(7):1461–1475
13. Emanuela M, Arun R (2014) A survey on anti-spoofing schemes for fingerprint recognition systems. *ACM Comput Surv* 47(2):36
14. Galbally J, Gomez-Barrero M (2016) A review of iris anti-spoofing. In: 4th IEEE international workshop on biometrics and forensics (IWBF), pp 1–6
15. Galbally Herrero J, Fierrez J, Ortega-García J (2007) Vulnerabilities in biometric systems: attacks and recent advances in liveness detection. in *Proc. Spanish Workshop on Biometrics* 1(3):1–8
16. Galbally J, Alonso-Fernandez F, Fierrez J, Ortega-Garcia J (2009) Fingerprint liveness detection based on quality measures. In: Proceedings of IEEE international conference on biometrics, identity and security, pp 1–8
17. Galbally J, Alonso-Fernandez F, Fierrez J, Ortega-Garcia J (2012) A high performance fingerprint liveness detection method based on quality related features. *Futur Gener Comput Syst* 28(1):311–321
18. Galbally J, Ortiz-Lopez J, Julian F, Ortega-Garcia J (2012) Iris liveness detection based on quality related features. In: Proceedings of 5th IEEE international conference on biometrics, pp 271–276
19. Galbally J, Marcel S, Fierrez J (2014) Image quality assessment for fake biometric detection: application to iris, fingerprint, and face recognition. *IEEE Trans Image Process* 23(2):710–724
20. Ghiani L, Marcialis GL, Roli F (2012) Fingerprint liveness detection by local phase quantization. In: Proceedings of 21st IEEE international conference on pattern recognition, pp 537–540

21. Gomez-Barrero M, Galbally J, Fierrez J (2014) Efficient software attack to multimodal biometric systems and its application to face and iris fusion. *Pattern Recogn Lett* 36:243–253
22. Gottschlich C, Mikaelyan A, Olsen MA, Bigun J, Busch C (2015) Improving fingerprint alteration detection. In: *Proceedings of 9th IEEE international symposium on in image and signal processing and analysis (ISPA)*, pp 83–86
23. Gragnaniello D, Poggi G, Sansone C, Verdoliva L (2015) Local contrast phase descriptor for fingerprint liveness detection. *Pattern Recogn* 48(4):1050–1058
24. Haralick RM, Shanmugam K, Dinstein IH (1973) Textural features for image classification. *IEEE Trans Syst Man Cybern* 3(6):610–621
25. Hezil N, Boukrouche A (2017) Multimodal biometric recognition using human ear and palmprint. *IET Biometrics* 6(5):351–359
26. Hu Y, Sirlantzis K, Howells G (2016) Iris liveness detection using regional features. *Pattern Recogn Lett* 82: 242–250
27. Jain AK, Ross A, Prabhakar S (2004) An introduction to biometric recognition. *IEEE Trans Circuits Syst Video Technol* 14(1):4–20
28. Jain A, Nandakumar K, Ross A (2005) Score normalization in multimodal biometric systems. *Pattern Recogn Lett* 38:2270–2285
29. Jia J, Cai L (2007) Fake finger detection based on time-series fingerprint image analysis. In: *Proceedings of international conference on intelligent computing*, pp 1140–1150
30. Johar T, Kaushik P (2015) Iris segmentation and normalization using Daugman’s rubber sheet model. *Int J Sci Tech Adv* 1(1):11–14
31. Kohli N, Yadav D, Vatsa M, Singh R, Noore A (2016) Detecting medley of iris spoofing attacks using DESIST. In: *Proceedings of 8th international conference on biometrics theory, applications and systems*, pp 1–6
32. Marasco E, Sansone C (2012) Combining perspiration-and morphology-based static features for fingerprint liveness detection. *Pattern Recogn Lett* 33(9):1148–1156
33. Memon S, Manivannan N, Balachandran W (2011) Active pore detection for liveness in fingerprint identification system. In: *Proceedings of 19th IEEE telecommunications forum (TELFOR)*, pp 619–622
34. Nandakumar K, Chen Y, Dass SC, Jain A (2008) Likelihood ratio based biometric score fusion. *IEEE Trans Pattern Anal Mach Intell* 30(2):342–347
35. Nguyen K, Denman S, Sridharan S, Fookes C (2015) Score-level multibiometric fusion based on Dempster–Shafer theory incorporating uncertainty factors. *IEEE Trans Hum-Mach Syst* 45(1):132–140
36. Nikam SB, Agarwal S (2008) Local binary pattern and wavelet-based spoof fingerprint detection. *Int J Biometrics* 1(2):141–159
37. Nikam SB, Agarwal S (2010) Curvelet-based fingerprint anti-spoofing. *SIViP* 4(1):75–87
38. Nogueira RF, de Alencar Lotufo R, Machado RC (2016) Fingerprint Liveness detection using convolutional neural networks. *IEEE Trans Inf Forensics Secur* 11(6):1206–1213
39. Oloyede MO, Hancke GP (2016) Unimodal and multimodal biometric sensing systems: a review. *IEEE Access* 4:7532–7555
40. Poh N, Kittler J, Bourli T (2010) Quality-based score normalization with device qualitative information for multimodal biometric fusion. *IEEE Trans Syst Man Cybern Part A Syst Hum* 40(3):539–554
41. Raghavendra R, Busch C (2015) Robust scheme for iris presentation attack detection using multiscale binarized statistical image features. *IEEE Trans Inf Forensics Secur* 10(4):703–715
42. Ratha NK, Connell JH, Bolle RM (2001) Enhancing security and privacy in biometrics-based authentication systems. *IBM Syst J* 40(3):614–634
43. Ross A, Jain AK (2003) Information fusion in biometrics. *Pattern Recogn Lett* 24(13):2115–2125
44. Shafer G (1976) *A mathematical theory of evidence*. Princeton University Press, Princeton
45. Singh YN, Singh SK (2013) A taxonomy of biometric system vulnerabilities and defences. *Int J Biometrics* 5(2):137–159
46. Toth B (2005) Biometric liveness detection. *Inf Secur Bull* 10(8):291–297
47. Vora A, Paunwala CN, Paunwalla M (2014) Statistical analysis of various kernel parameters on SVM based multimodal fusion. In: *Proceedings of IEEE India conference*, pp 1–5
48. Wang S, Gu K, Zeng K, Wang Z, Lin W (2018) Objective quality assessment and perceptual compression of screen content images. *IEEE Comput Graph Appl* 38(1):47–58
49. Wild P, Radu P, Chen L, Ferryman J (2016) Robust multimodal face and fingerprint fusion in the presence of spoofing attacks. *Pattern Recogn Lett* 50:17–25
50. Yadav D, Kohli N, Doyle JS, Singh R, Vatsa M, Bowyer KW (2014) Unraveling the effect of textured contact lenses on iris recognition. *IEEE Trans Inf Forensics Secur* 9(5):851–862
51. Yambay D, Ghiani L, Denti P, Marcialis GL, Roli F, Schuckers S (2012) LivDet 2011—fingerprint liveness detection competition 2011. In: *Proceedings of 5th IEEE international conference on biometrics*, pp 208–215

52. Yan C, Wang ZZ, Gao QB, Du YH (2005) A novel kernel for sequences classification. In: Proceedings of IEEE international conference on natural language processing and knowledge engineering, pp 769–773
53. Yuan C, Li X, Wu QJ, Li J, Sun X (2017) Fingerprint liveness detection from different fingerprint materials using convolutional neural network and principal component analysis. *Comput Mater Continua* 53(4):357–372

**Publisher's note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Rohit Agarwal** received the M.Tech. degree in Computer Science from UPTU Lucknow, India. He is pursuing the Ph.D. in the area of Computer Vision from GLA University Mathura, India. He has 15 years of teaching experience and currently, he is working as an Assistant Professor in Department of Computer Engineering and Applications, GLA University, Mathura, India. His research interests include Image Processing and Computer Vision.



**Anand Singh Jalal** received the M.Tech degree in Computer Science from Devi Ahilya Vishwavidyalaya, Indore, India. He received the PhD in the area of Computer Vision from Indian Institute of Information Technology (IIIT), Allahabad, India. He has 19 years of teaching and research experience and currently, he is working as a Professor in Department of Computer Engineering and Applications, GLA University, Mathura, India. His research interests include Image Processing, Computer Vision and Pattern Recognition.





**K. V. Arya** achieved the Master of Engineering (ME) degree in Electrical Engineering from Indian Institute of Science (IISc), Bangalore, India and earned Ph. D. degree in Computer Science & Engineering from Indian Institute of Technology, Kanpur, India. He has more than 27 years teaching experience and published more than 150 journal and conference papers. He is senior member of IEEE, fellow of IETE, fellow of Institution of Engineers (India), member of ACM and life member of IFTE. Currently, he is working as Professor in Department of Computer Science & Engineering, IET Lucknow, India. His research interests include Biometrics, Image Processing, Computer Vision and Reliability Analysis.